

**Information Sheet for preparing an Information
Disclosure Statement under Rule 1.56**

Suzuye Ref.03S0936

Foreign Patent Documents

Document No.: 2000-76402, published **March 14, 2000**

Country: **Japan**

Copy of reference: **attached**

Language: **non-English**

English translation: **not attached for it is not readily available**

Concise Explanation of Pertinency: **This publication is referred to in
the specification. See page 2, line 7.**

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-76402

(P2000-76402A)

(43) 公開日 平成12年3月14日 (2000.3.14)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
G 0 6 K 19/073		G 0 6 K 19/00	P 5 B 0 1 7
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 C 5 B 0 3 5
G 0 6 K 17/00		G 0 6 K 17/00	E 5 B 0 5 8

審査請求 未請求 請求項の数 3 O L (全 4 頁)

(21) 出願番号 特願平10-243071

(22) 出願日 平成10年8月28日 (1998.8.28)

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 矢野義博

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(72) 発明者 半田富己男

東京都新宿区市谷加賀町一丁目1番1号大

日本印刷株式会社内

(74) 代理人 100092495

弁理士 蛭川 昌信 (外7名)

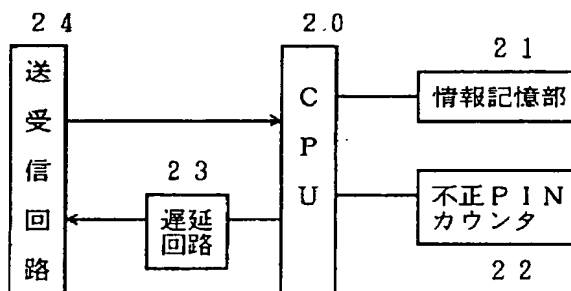
最終頁に続く

(54) 【発明の名称】 レスポンスタイムを可変化したICカード

(57) 【要約】

【課題】 総当たり攻撃からPINの類推を不可能にし、セキュリティを向上させる。

【解決手段】 情報記録手段21と情報処理制御手段20とを持ち、情報処理制御手段20により外部から入力された命令を解釈し、情報記録手段21にアクセスして一定の処理を行ってレスポンスを返すICカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段23を設けたものである。



1

【特許請求の範囲】

【請求項1】 情報記録手段と情報処理制御手段とを持ち、前記情報処理制御手段により外部から入力された命令を解釈し、情報記録手段にアクセスして一定の処理を行ってレスポンスを返すICカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段を設けたことを特徴とするレスポンスタイムを可変化したICカード。

【請求項2】 利用者コードの照合命令、または認証コードの認証命令が連続し、所定回数に達したことを条件に前記遅延手段によりレスポンスを遅延させるようにしたことを特徴とする請求項1記載のレスポンスタイムを可変化したICカード。

【請求項3】 前記遅延手段は、照合命令または認証命令の回数が所定値に達する毎に階段状に遅延時間を増大させることを特徴とする請求項2記載のレスポンスタイムを可変化したICカード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はICカードと端末装置間の通信において、端末装置より入力される命令に対するICカードからのレスポンスの送信タイミングを可変化するようにしたICカードに関する。

【0002】

【従来の技術】従来、ICカードの不正利用に対する防止策として外部からの命令に対するICカードのレスポンス時間に着目したものが知られている。例えば、特開昭62-251963号公報は、Personal Identification Number（以下PIN）の照合のためのレスポンス時間をあえて一定にするもので、これはPINが正しいか、間違っているかを判断するとき、判断するロジックが変わるとレスポンス時間が変化し、そのためロジックの類推が可能となるので、あえてレスポンス時間を一定にすることで、悪意のある者からのロジックの類推を防ぐように工夫したものである。

【0003】また、特開平10-69222号公報では、ICカード内で暗号化処理、復号処理を行うものにおいて、暗号化のために使用した鍵とレスポンス時間とが相関をもち、レスポンス時間から鍵の性質が分かる可能性があるため、レスポンス時間をランダムに遅延させることにより鍵の類推を防止している。

【0004】

【発明が解決しようとする課題】ICカードの情報記録部あるいはアクセス制御部へのアクセスのためのコマンドに対するICカードからのレスポンスのタイミングは、照合や認証の正否等の結果や、レスポンスに載せる情報生成手順によって異なるが、同じ処理手順で行う場合、処理に要する時間はほぼ一定になる傾向がある。例えば、ICカードのような高セキュリティな機能を有す

2

る媒体において、不正な利用者によるランダムなPIN入力に対しても照合結果の出力に要する時間は正当な利用者のものと変わらず、そのため総当たり攻撃によってPINが分かってしまう可能性がある。

【0005】本発明は上記課題を解決するためのもので、総当たり攻撃からPINや認証用暗号鍵の類推を不可能にし、セキュリティを向上させることを目的とする。

【0006】

【課題を解決するための手段】本発明は、情報記録手段と情報処理制御手段とを持ち、前記情報処理制御手段により外部から入力された命令を解釈し、情報記録手段にアクセスして一定の処理を行ってレスポンスを返すICカードにおいて、前記レスポンスのタイミングを遅延させる遅延手段を設けたことを特徴とする。また本発明は、利用者コードの照合命令または認証コードの認証命令が連続し、所定回数に達したことを条件に遅延手段によりレスポンスを遅延させるようにしたことを特徴とする。また本発明は、遅延手段は、照合命令または認証命令の回数が所定値に達する毎に階段状に遅延時間を増大させることを特徴とする。

【0007】

【発明の実施の形態】以下、本発明の実施の形態について説明する。図1は本発明のシステム概念図で、端末装置1に対してICカード2をセットすると、端末装置1からはICカード2に対して、コマンド（命令）を送信し、これを受信したICカード2はコマンドを解釈して書き込み、読み取り、読み出し等の処理を実行し、処理結果をレスポンスとして端末装置1に返すようになっている。

【0008】図2は本発明のICカードの構成を示す概念図である。ICカードにはCPU20、情報記憶部21、不正PINカウンタ22、遅延回路23、送受信回路24を有している。情報記憶部21はプログラム記憶領域、作業エリア、書換え可能な不揮発性メモリ領域を有している。CPU20は、端末装置1から送信されるコマンドを受信するとコマンドと共に送信されたデータを読み込み、情報記憶部21にアクセスして必要な処理を行い、結果を送受信回路24よりレスポンスとして出力する。さらに本発明においては、不正PINカウンタ22、遅延回路23を有している。不正PINカウンタ22は連続してPIN入力が行われたとき、その入力された回数をカウントするものであり、遅延回路23はレスポンス時間を遅延させるためのものである。遅延手段は、遅延回路ではソフトウェアによる実現のいずれでもよい。

【0009】図3はICカードの信号の流れを示しており、図示するように、送受信回路24を通してPIN入力が行われると、CPU20では入力したPINが真正か否かを判定するための照合を行い、正否を送受信回路

3

24を通してレスポンスとして送信する。不正PINカウンタ22は連続して入力される不正なPIN入力回数をカウントし、例えば、図4に示すように、不正PIN入力回数が所定値に達すると、所定の遅延時間を遅延回路23に設定する。この不正PIN入力回数に対して階段状に遅延時間が増えるように設定する。このため、総当たり攻撃でPIN入力を行おうとすると、入力回数に応じて応答時間が飛躍的にかかってしまうため、結局は真正なPIN情報を盗み取ることは不可能である。

【0010】図5はレスポンスを遅延させる処理フロー10を示す図である。PIN入力があってこれを受信すると(S1)、入力されたPINが真正か否か判断するための照合を行う(S2)。照合の結果、真正なものであれば次の処理に進み、真正でないと判断されると不正PINカウンタをインクリメントする(S3、S4)。次いで、不正PINカウンタの値が所定値K以上か否か判断し(S5)、所定値K未満であれば、通常のタイミングでPINが間違っていることをレスポンスとして出力し(S7)、所定値K以上であればレスポンスの時間を遅

4

*延させ(S6)、出力する。

【0011】

【発明の効果】以上のように本発明によれば、連続的に入力される不正なPIN入力に対し、ICカードからのレスポンス送信までの時間を大幅に遅らせことによりランダムなPIN入力による総当たり攻撃を防ぐことが可能となる。

【図面の簡単な説明】

【図1】 本発明のシステム概念図である。

【図2】 本発明のICカードの構成を示す図である。

【図3】 ICカードの信号の流れを示す図である。

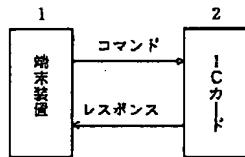
【図4】 不正PIN入力回数に対する遅延時間の関係を示す図である。

【図5】 レスポンスを遅延させる処理フローを示す図である。

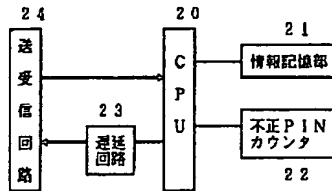
【符号の説明】

1…端末装置、2…ICカード、20…CPU、21…情報記憶部、22…不正PINカウンタ、23…遅延回路、24…送受信回路。

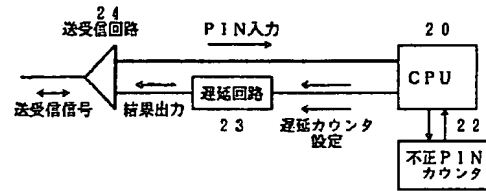
【図1】



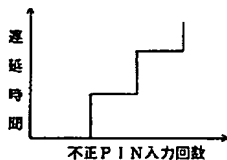
【図2】



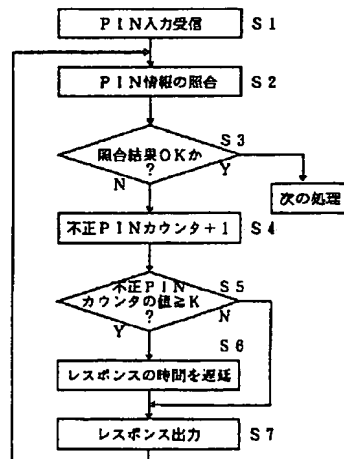
【図3】



【図4】



【図5】



フロントページの続き

(72)発明者 松田雅之

東京都新宿区市谷加賀町一丁目 1 番 1 号大
日本印刷株式会社内

(72)発明者 柴田直人

東京都新宿区市谷加賀町一丁目 1 番 1 号大
日本印刷株式会社内

F ターム(参考) 5B017 AA01 BA05 BB02 BB03 BB10
CA14
5B035 AA14 BB09 CA12
5B058 CA27 KA33